CDC Secure Data Network User Enrollment Guide (Internet Explorer)

Overview

This document provides an overview of the enrollment process of the CDC Secure Data Network (SDN) using Microsoft® Internet Explorer. **Specific instructions for completing enrollment in the Hospital Smallpox Vaccine Monitoring System (HSVMS) are shown in large text throughout the document.**

Access Enrollment Site

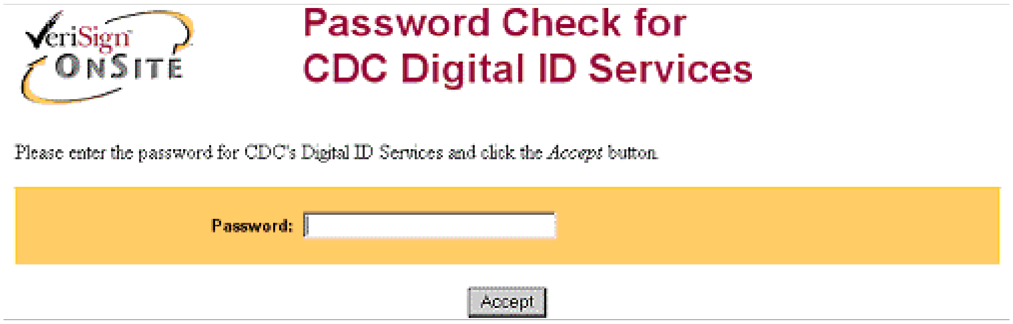
To begin the enrollment process, you must first access the SDN enrollment website.

You must access the SDN enrollment website and complete the enrollment process from the same computer and browser you will be using to access SDN.

The website can be reached by accessing the following uniform resource locator (URL):

https://ca.cdc.gov

Upon accessing this site, a page similar to the one below will appear. To continue, you must enter the general registration password that should have been provided by your program administrator. Please note that this password cannot be provided in this document for security purposes, nor can CDC SDN Support provide it. After you enter the registration password, click on the Accept button to continue.

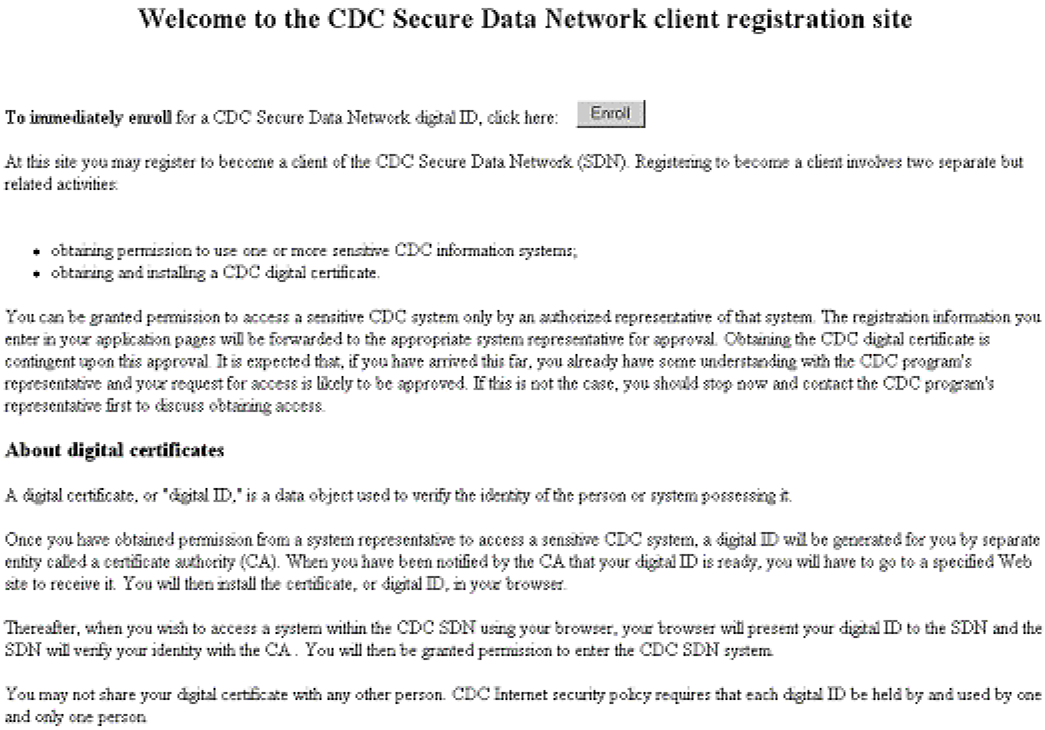


Password Check for
CDC Digital ID Services

Please enter the password for CDC's Digital ID Services and click the *Accept* button.

Review Enrollment Information

After authentication, you will be presented with a general information page providing an overview of digital certificates and system requirements. After you review the enrollment information, proceed to the first enrollment step by clicking the Enroll button.



Welcome to the CDC Secure Data Network client registration site

To immediately enroll for a CDC Secure Data Network digital ID, click here: Enroll

At this site you may register to become a client of the CDC Secure Data Network (SDN). Registering to become a client involves two separate but related activities:

- obtaining permission to use one or more sensitive CDC information systems;
- obtaining and installing a CDC digital certificate.

You can be granted permission to access a sensitive CDC system only by an authorized representative of that system. The registration information you enter in your application pages will be forwarded to the appropriate system representative for approval. Obtaining the CDC digital certificate is contingent upon this approval. It is expected that, if you have arrived this far, you already have some understanding with the CDC program's representative and your request for access is likely to be approved. If this is not the case, you should stop now and contact the CDC program's representative first to discuss obtaining access.

About digital certificates

A digital certificate, or "digital ID," is a data object used to verify the identity of the person or system possessing it.

Once you have obtained permission from a system representative to access a sensitive CDC system, a digital ID will be generated for you by separate entity called a certificate authority (CA). When you have been notified by the CA that your digital ID is ready, you will have to go to a specified Web site to receive it. You will then install the certificate, or digital ID, in your browser.

Thereafter, when you wish to access a system within the CDC SDN using your browser, your browser will present your digital ID to the SDN and the SDN will verify your identity with the CA . You will then be granted permission to enter the CDC SDN system.

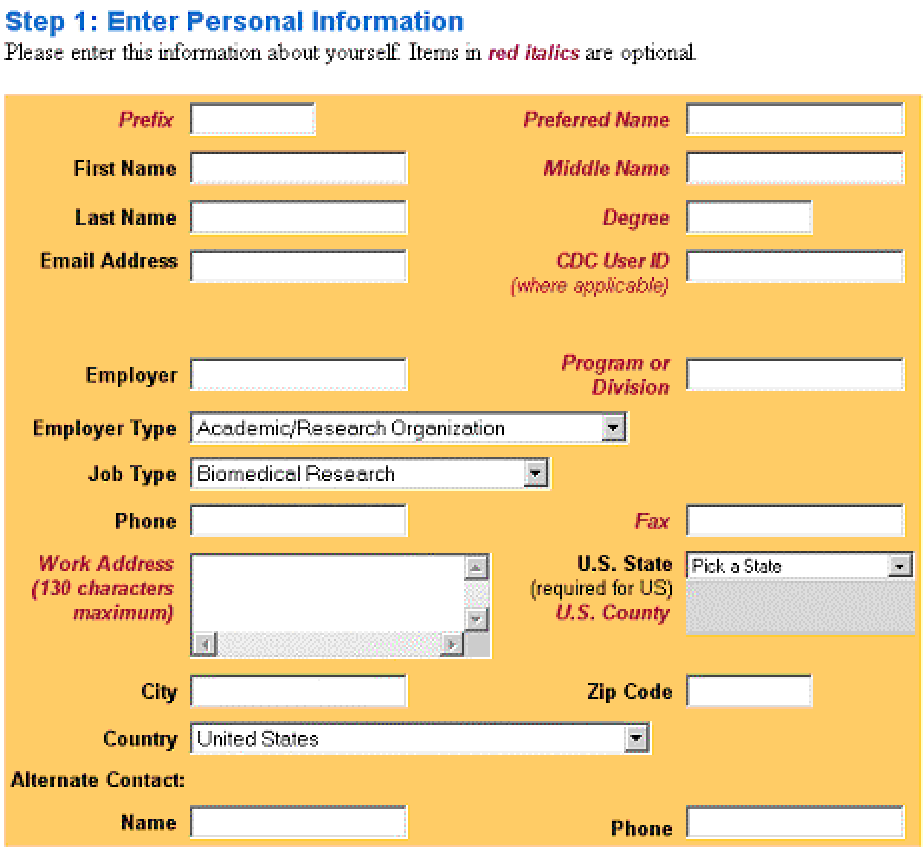
You may not share your digital certificate with any other person. CDC Internet security policy requires that each digital ID be held by and used by one and only one person.

Enter Personal Information

The top part of the page contains an option for a non-Java version of the application as well as important information about your browser. **Click on “Non-Java Page”.**

To enroll for a digital certificate, your version of Internet Explorer must be 4.x or higher.

Below the information area is a form that must be completed to continue the enrollment process. The form is used to create your digital certificate and should be completed with as much information as possible (all optional information is identified by red italics). The HSVMS program administrator at CDC will use this information to verify your identity.
IMPORTANT: If your facility is a hospital, enter your unique facility ID (e.g., CMS Provider #, VA Station Code) into the "Program or Division" box. We cannot process your request for a digital certificate without this number.



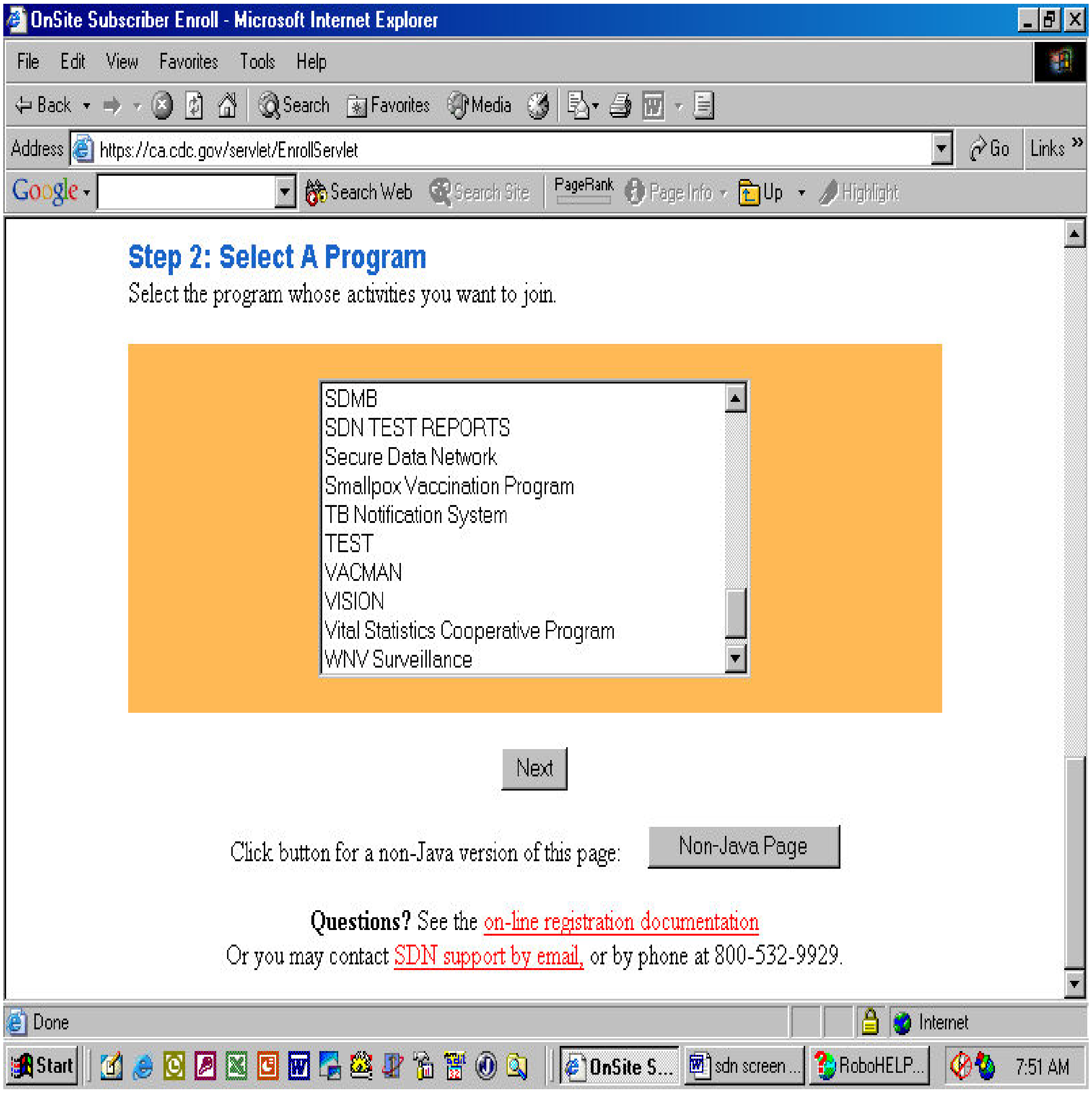
Step 1: Enter Personal Information

Please enter this information about yourself. Items in *red italics* are optional.

Prefix		*Preferred Name*	
First Name		*Middle Name*	
Last Name		*Degree*	
Email Address		*CDC User ID* *(where applicable)*	
Employer		*Program or Division*	
Employer Type	Academic/Research Organization		
Job Type	Biomedical Research		
Phone		*Fax*	
Work Address (130 characters maximum)		U.S. State (required for US) *U.S. County*	Pick a State
City		Zip Code	
Country	United States		
Alternate Contact:			
Name		Phone	

Select Program

The list box below the personal information form allows you to choose the program for which you are requesting access. To select the program, simply highlight the appropriate entry in the list box. Select **Smallpox Vaccination Program** from the list presented.


OnSite Subscriber Enroll - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://ca.cdc.gov/servlet/EnrollServlet
Go Links
Google Search Web Search Site PageRank Page Info Up Highlight
Done
Internet
Start OnSite S... sdn screen ... RoboHELP... 7:51 AM

Step 2: Select A Program

Select the program whose activities you want to join.

SDMB
SDN TEST REPORTS
Secure Data Network
Smallpox Vaccination Program
TB Notification System
TEST
VACMAN
VISION
Vital Statistics Cooperative Program
WNV Surveillance

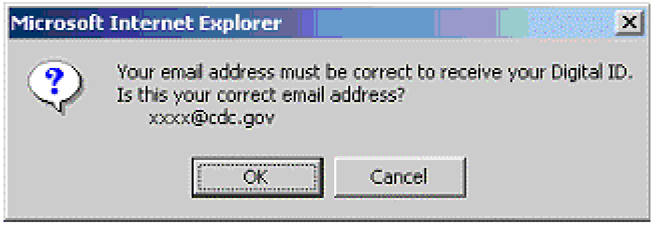
Next

Click button for a non-Java version of this page: Non-Java Page

Questions? See the on-line registration documentation
Or you may contact SDN support by email, or by phone at 800-532-9929.

Upon initial enrollment, you may select only one program from the available list. If you require access to more than one program, select the program identified by your program administrator. After obtaining your digital certificate, you will be able to request additional programs and activities via SDN (it is not necessary to apply for more than one digital certificate).

After completing the personal information form and selecting the program to which you are applying, click the "Next" button to continue. A confirmation dialog box will appear to verify the E-mail address provided on the personal information form.

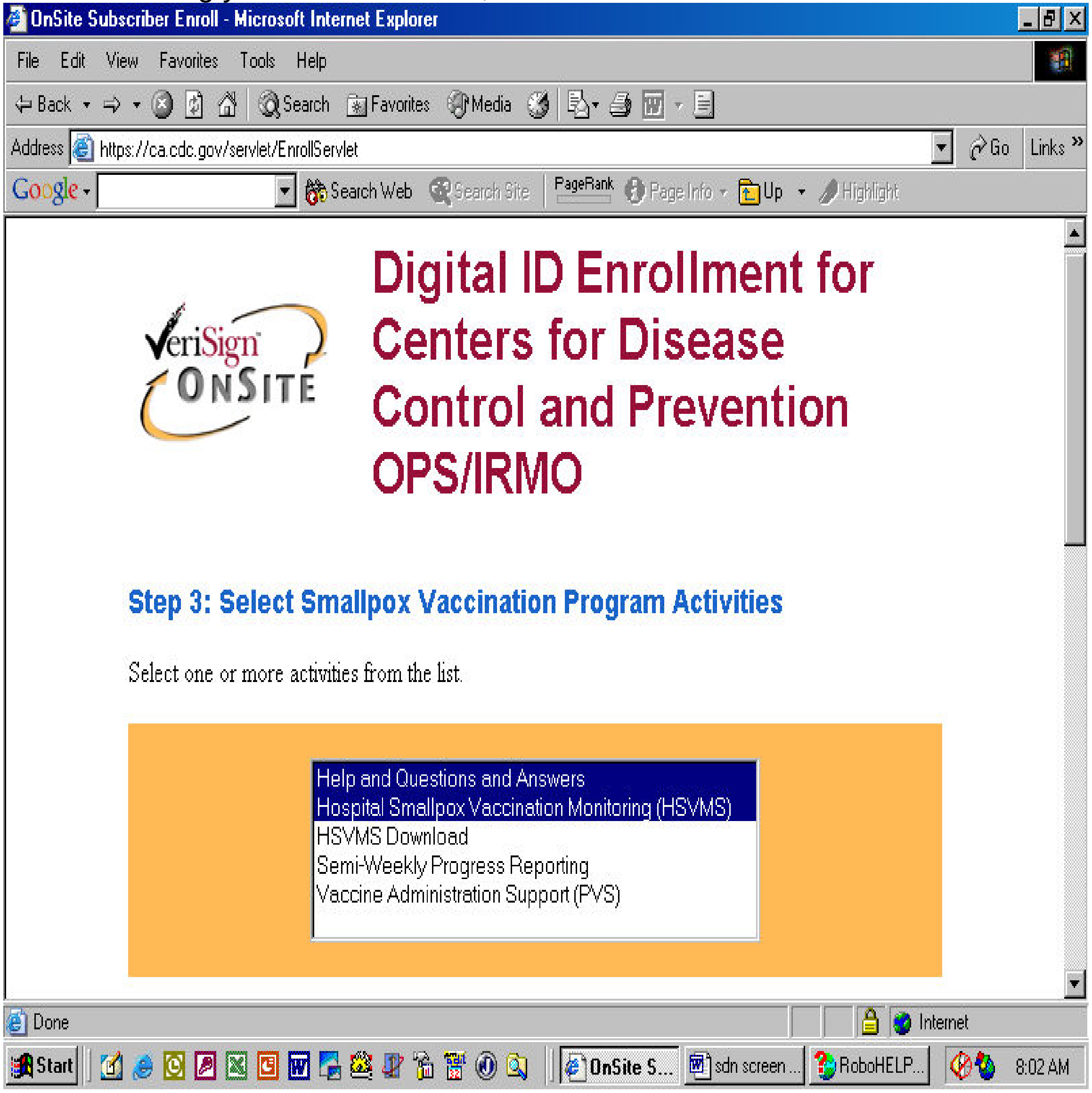


Microsoft Internet Explorer

Your email address must be correct to receive your Digital ID.
Is this your correct email address?
xxxx@cdc.gov

It is important that the Email address you provide is accurate and used in conjunction with the performance of your duties (i.e., not a personal account). The information required to complete the installation of your digital certificate will be sent to the address provided.

After confirming your Email address, click the OK button to continue.



OnSite Subscriber Enroll - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://ca.cdc.gov/servlet/EnrollServlet
Go Links
Google Search Web Search Site PageRank Page Info Up Highlight
VeriSign OnSite

Digital ID Enrollment for Centers for Disease Control and Prevention OPS/IRMO

Step 3: Select Smallpox Vaccination Program Activities

Select one or more activities from the list.

Help and Questions and Answers
Hospital Smallpox Vaccination Monitoring (HSVMS)
HSVMS Download
Semi-Weekly Progress Reporting
Vaccine Administration Support (PVS)

Done
Internet
Start
OnSite S...
sdn screen ...
RoboHELP...
8:02 AM

Specify County

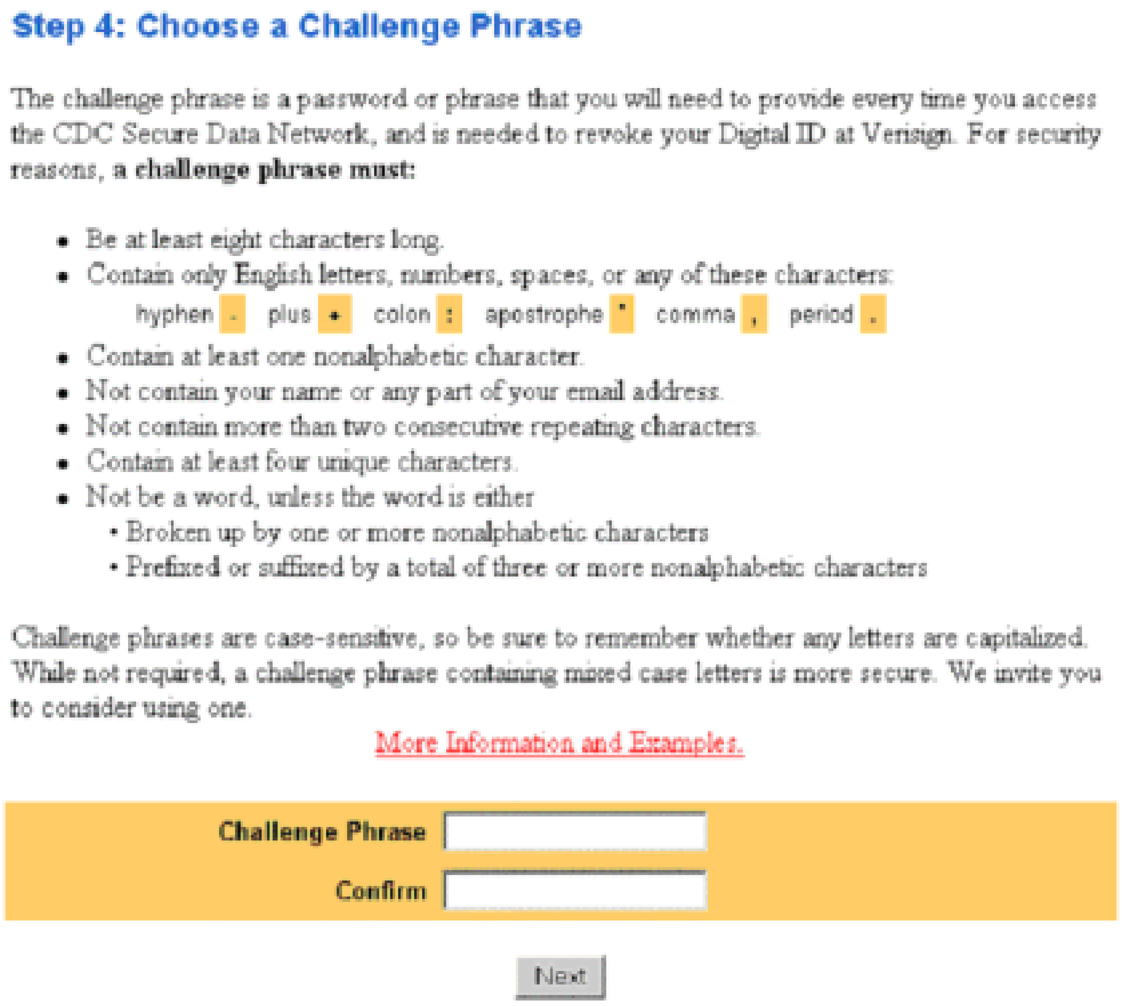
This is an optional step. You may highlight the county for your work address or skip to Step 4.

Select Smallpos Vaccination Program Activities

Click on Hospital Smallpox Vaccination Monitoring (HSVMS)

Choose a Challenge Phrase

Below the list of activities is a general overview of the challenge phrase that is required for use and management of your digital certificate. You must select a challenge phrase based on the guidelines presented and enter it twice (once in the “Challenge Phrase” field and once in the “Confirm” field). After you enter your challenge phrase in both fields, click the "Next" button to continue. **Choose a challenge phrase that you can remember as you will need it every time you want to access HSVMS.**



Step 4: Choose a Challenge Phrase

The challenge phrase is a password or phrase that you will need to provide every time you access the CDC Secure Data Network, and is needed to revoke your Digital ID at Verisign. For security reasons, **a challenge phrase must:**

- Be at least eight characters long.
- Contain only English letters, numbers, spaces, or any of these characters:
  hyphen - plus + colon : apostrophe ' comma , period .
- Contain at least one nonalphabetic character.
- Not contain your name or any part of your email address.
- Not contain more than two consecutive repeating characters.
- Contain at least four unique characters.
- Not be a word, unless the word is either
  - Broken up by one or more nonalphabetic characters
  - Prefixed or suffixed by a total of three or more nonalphabetic characters

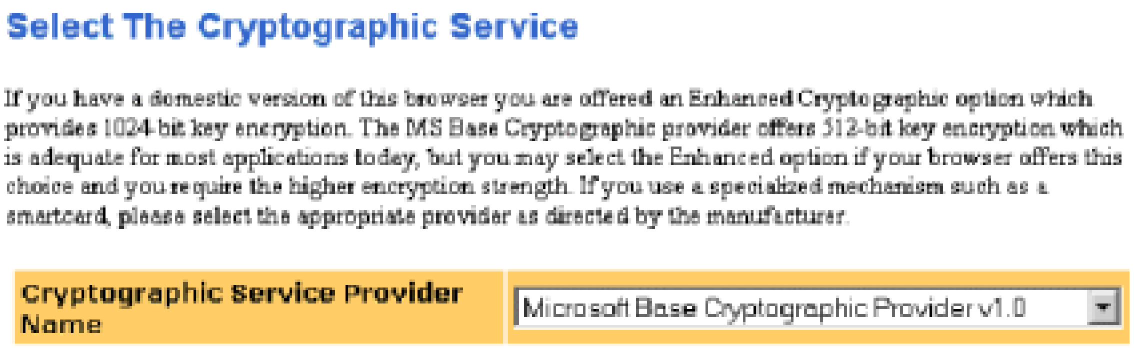
Challenge phrases are case-sensitive, so be sure to remember whether any letters are capitalized. While not required, a challenge phrase containing mixed case letters is more secure. We invite you to consider using one.

More Information and Examples.

Challenge Phrase	
Confirm	

Select Cryptographic Service

The Cryptographic Service Provider (CSP) is used to generate the digital certificate and determines the "cipher strength" employed. Because greater cipher strength is more desirable for transaction security, you should choose the strongest CSP available. **Choose the default selection as displayed.**



Select The Cryptographic Service

If you have a domestic version of this browser you are offered an Enhanced Cryptographic option which provides 1024-bit key encryption. The MS Base Cryptographic provider offers 512-bit key encryption which is adequate for most applications today, but you may select the Enhanced option if your browser offers this choice and you require the higher encryption strength. If you use a specialized mechanism such as a smartcard, please select the appropriate provider as directed by the manufacturer.

Cryptographic Service Provider Name	Microsoft Base Cryptographic Provider v1.0

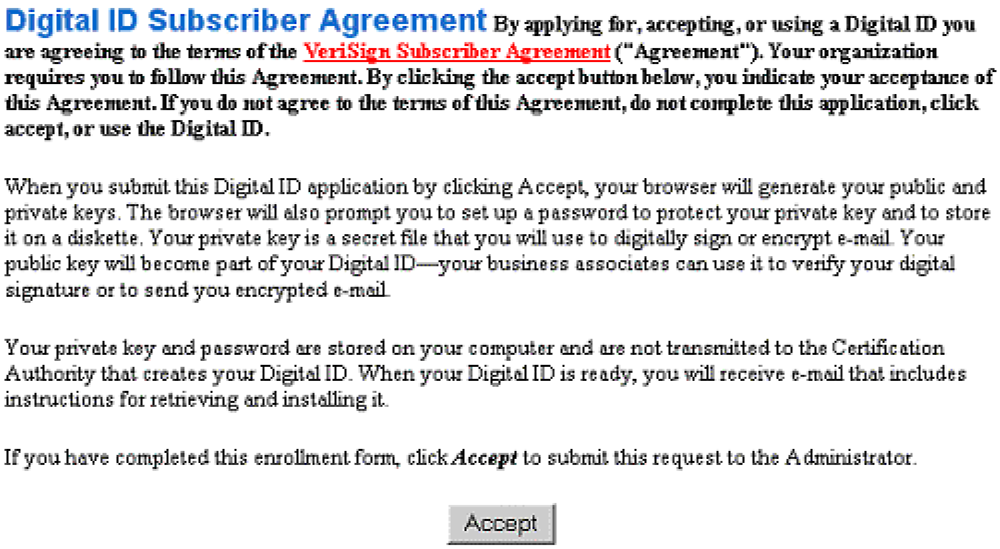
The CSP you choose should be based on the following priority (the available CSPs may vary):

1. Microsoft Strong Cryptographic Provider
2. Microsoft Enhanced Cryptographic Provider
3. Microsoft Basic Cryptographic Provider

If you are employing "smart card" technology and wish to use it in conjunction with your digital certificate, you will need to select the CSP based on the manufacturer's specifications.

Review and Accept Subscriber Agreement

After choosing your CSP, you are required to review and accept the VeriSign Subscriber Agreement before your digital certificate can be issued. The VeriSign Certification Practice Statement (CPS) governs the issuance and use of a digital certificate from VeriSign.



Digital ID Subscriber Agreement **By applying for, accepting, or using a Digital ID you are agreeing to the terms of the VeriSign Subscriber Agreement ("Agreement"). Your organization requires you to follow this Agreement. By clicking the accept button below, you indicate your acceptance of this Agreement. If you do not agree to the terms of this Agreement, do not complete this application, click accept, or use the Digital ID.**

When you submit this Digital ID application by clicking Accept, your browser will generate your public and private keys. The browser will also prompt you to set up a password to protect your private key and to store it on a diskette. Your private key is a secret file that you will use to digitally sign or encrypt e-mail. Your public key will become part of your Digital ID—your business associates can use it to verify your digital signature or to send you encrypted e-mail.

Your private key and password are stored on your computer and are not transmitted to the Certification Authority that creates your Digital ID. When your Digital ID is ready, you will receive e-mail that includes instructions for retrieving and installing it.

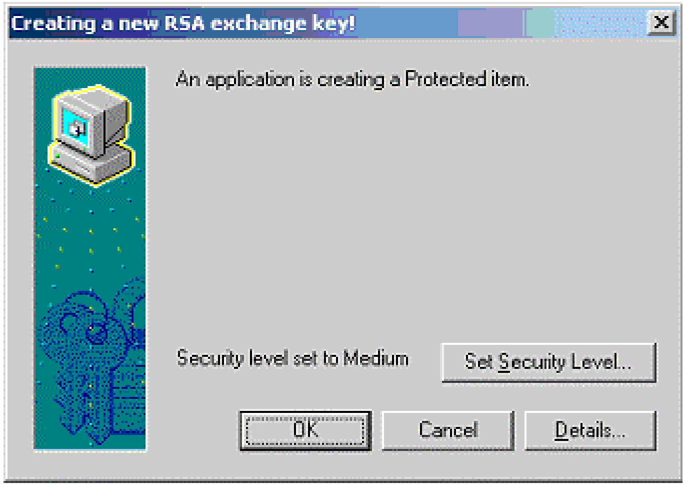
If you have completed this enrollment form, click ***Accept*** to submit this request to the Administrator.

For more information regarding the Agreement or CPS, please visit the VeriSign website at http://www.verisign.com/repository.

After you have reviewed the Agreement and agree to the terms presented, click the *Accept* button to continue.

Create an RSA Exchange Key

To begin the process of creating a digital certificate on your computer, you must generate a key request for submission to the certification authority (CA). Upon acceptance of the VeriSign Subscriber Agreement, Internet Explorer attempts to create a placeholder for the digital certificate. This placeholder is used to store information about the digital certificate request and allows the user to set a security level associated with use of the digital certificate.



An application is creating a Protected item.

Security level set to Medium

As part of the notification dialog box, a security level setting is displayed. An overview of each security level is as follows:

High – Internet Explorer prompts the user prior to use of the digital certificate and requires a password to be entered (this password may be different than the challenge phrase).

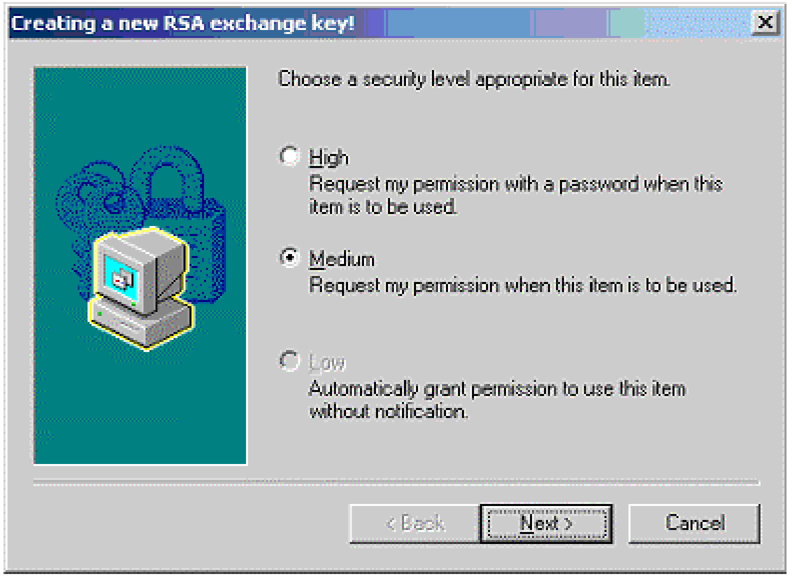
Medium – Internet Explorer prompts the user prior to the use of the digital certificate.

Low – Internet Explorer automatically uses the digital certificate without prompting the user.

If the current security level setting is "Low" or "Medium", and if either security level is acceptable for use of the digital certificate, click the OK button to continue and proceed to the "Check Email" section of this document.

Although a challenge phrase is required for SDN, the digital certificate itself does not require authentication for use. The digital certificate is stored on the local machine and information concerning it is created in the Windows Registry unique to the user currently logged-on. If multiple individuals use the same computer and/or local account, or if greater security associated with the digital certificate is desired, changing the security level may be necessary.

To change the security level to one other than that displayed by the dialog, click the Set Security Level button. A dialog box will appear presenting the available security levels.



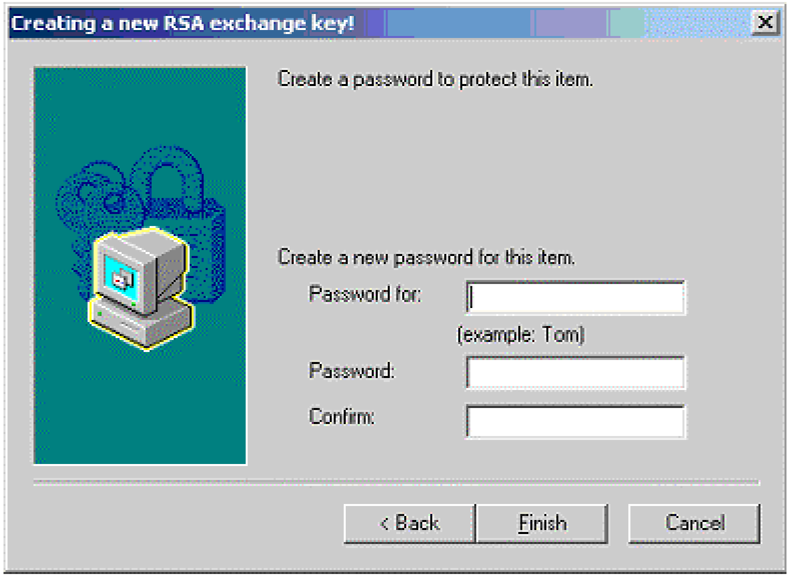
Choose a security level appropriate for this item.

○ High
Request my permission with a password when this item is to be used.

● Medium
Request my permission when this item is to be used.

○ Low
Automatically grant permission to use this item without notification.

To change the security level, click the radio button next to the appropriate selection; click the "Next >" button to continue. If the security level is set to “High”, a password dialog box will appear.



Create a password to protect this item.

Create a new password for this item.

Password for: |
(example: Tom)

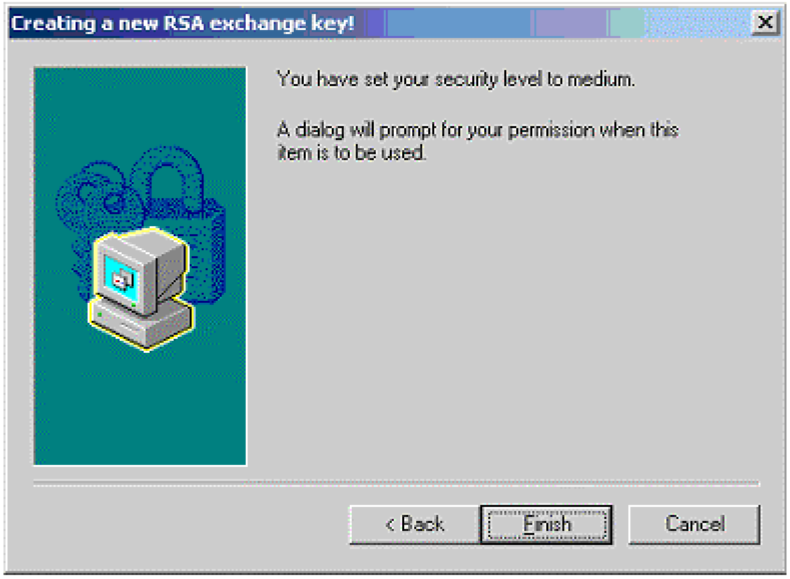
Password:

Confirm:

To establish a password for the digital certificate, enter an item name in the “Password for:” field (e.g., SDN) and a password (with confirmation) in the fields below.

The local password for protecting the digital certificate is not used by SDN and therefore cannot be recovered (changed) by SDN personnel. Additionally, the password constraints used for the SDN challenge phrase do not apply.

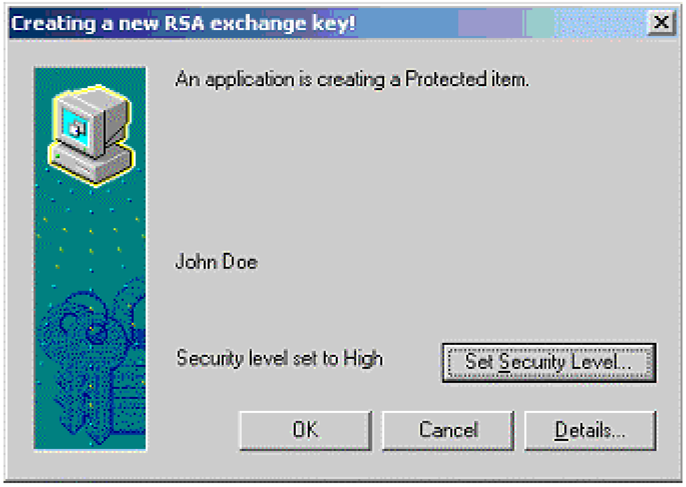
If the security level is set to “Medium”, a confirmation dialog box will appear.


Creating a new RSA exchange key!

You have set your security level to medium.

A dialog will prompt for your permission when this item is to be used.

If the security level is correct, click the "Finish" button to continue. If the security level is not correct, click the "< Back" button to return to the security level selection dialog box. After setting the security level, the original notification dialog box reappears and reflects any security level changes made.


Creating a new RSA exchange key!

An application is creating a Protected item.

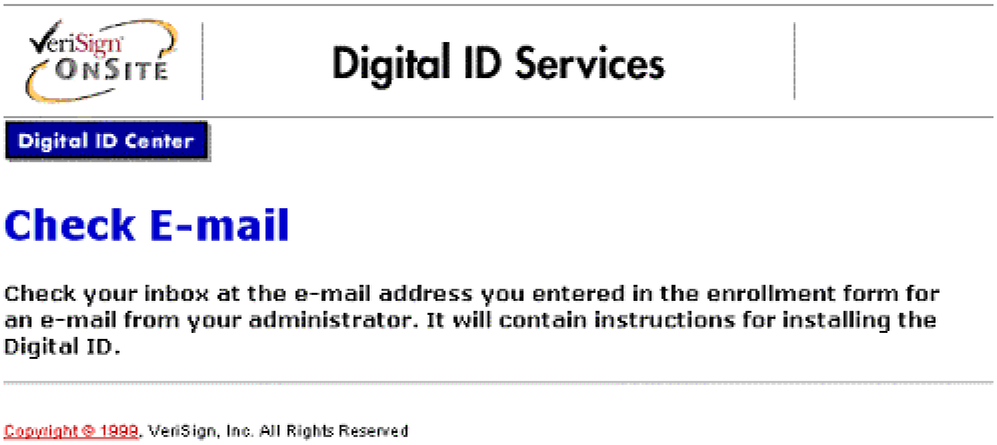
John Doe

Security level set to High

If the security level settings are correct, click the "OK" button to continue.

Check Email

Once the digital certificate placeholder has been created, a notification to check your Email account (the one provided during enrollment) will appear.



Check E-mail

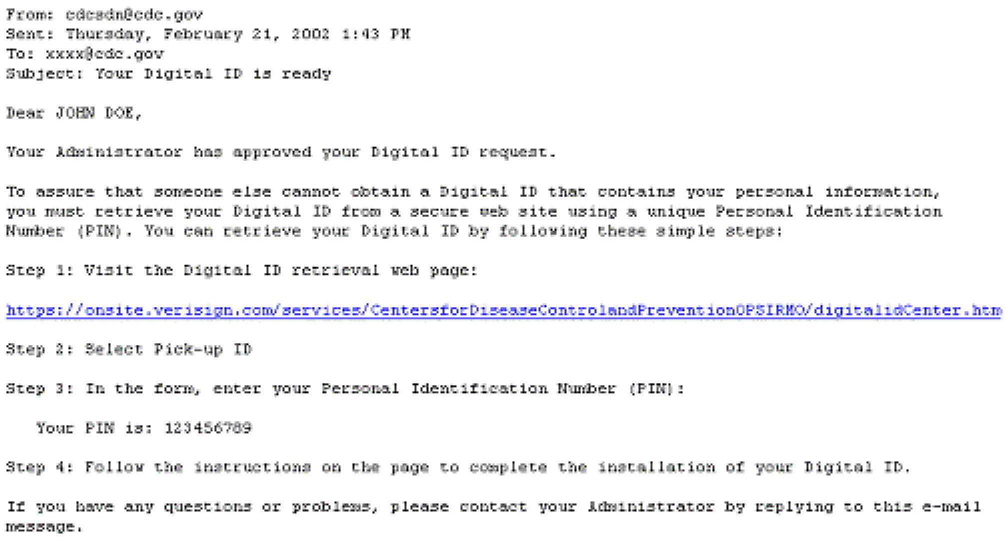
Check your inbox at the e-mail address you entered in the enrollment form for an e-mail from your administrator. It will contain instructions for installing the Digital ID.

Copyright © 1999, VeriSign, Inc. All Rights Reserved

Exit out of the SDN enrollment website now. Within a few hours or 48 hours at most, you should receive an email stating that your digital certificate request has been approved (see next page). Please do not call the support line until 48 working hours have passed (404-498-2110 or 1-800-532-9929). We anticipate receiving many requests for digital certificates and it will take some time to process them.

Digital Request Approval

Once your digital certificate request (including program activities) has been approved, an Email will be sent to your account with instructions and a personal identification number (PIN) for obtaining your digital certificate.



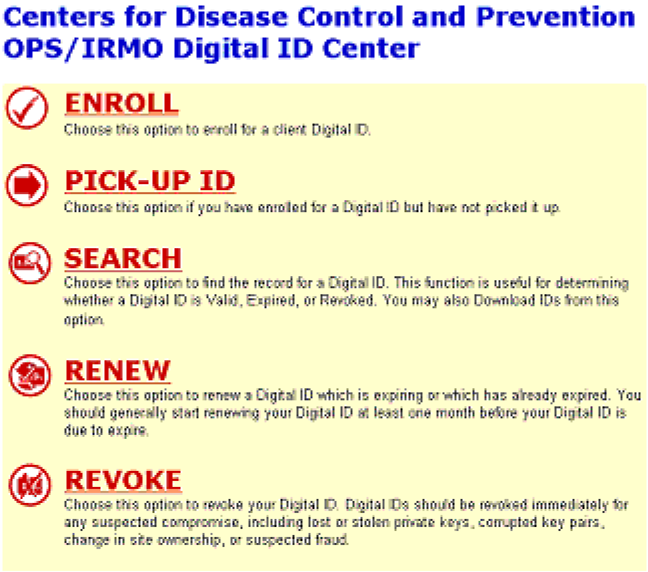
```
From: cdcsdn@cdc.gov
Sent: Thursday, February 21, 2002 1:43 PM
To: xxxx@cdc.gov
Subject: Your Digital ID is ready

Dear JOHN DOE,

Your Administrator has approved your Digital ID request.

To assure that someone else cannot obtain a Digital ID that contains your personal information,
you must retrieve your Digital ID from a secure web site using a unique Personal Identification
Number (PIN). You can retrieve your Digital ID by following these simple steps:

Step 1: Visit the Digital ID retrieval web page:

https://onsite.verisign.com/services/CentersforDiseaseControlandPreventionOPSIRMO/digitalidCenter.htm

Step 2: Select Pick-up ID

Step 3: In the form, enter your Personal Identification Number (PIN):

   Your PIN is: 123456789

Step 4: Follow the instructions on the page to complete the installation of your Digital ID.

If you have any questions or problems, please contact your Administrator by replying to this e-mail
message.
```

You must use the same computer and browser to pick-up your digital certificate as was used to complete the enrollment process. If a different browser or computer is used, the installation will fail (you will, however, be able to re-attempt the process using the correct browser and computer at a later time).

To complete the installation of your digital certificate, go to the URL provided in the Email notification.

If you manually enter the URL provided in the notification, you must use a secure HTTP session (i.e., https).

The notification URL will direct the browser to the VeriSign Digital ID Center for CDC.



Centers for Disease Control and Prevention
OPS/IRMO Digital ID Center

ENROLL
Choose this option to enroll for a client Digital ID.

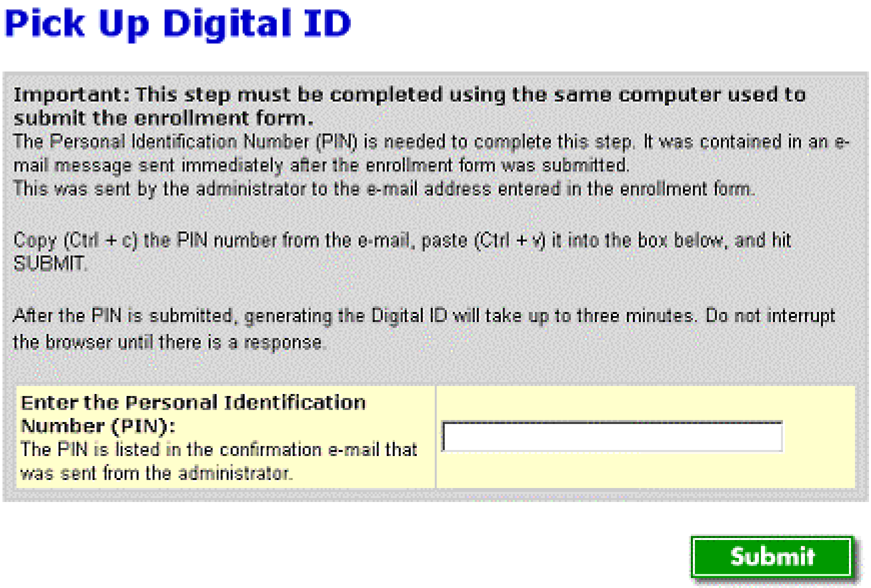
PICK-UP ID
Choose this option if you have enrolled for a Digital ID but have not picked it up.

SEARCH
Choose this option to find the record for a Digital ID. This function is useful for determining whether a Digital ID is Valid, Expired, or Revoked. You may also Download IDs from this option.

RENEW
Choose this option to renew a Digital ID which is expiring or which has already expired. You should generally start renewing your Digital ID at least one month before your Digital ID is due to expire.

REVOKE
Choose this option to revoke your Digital ID. Digital IDs should be revoked immediately for any suspected compromise, including lost or stolen private keys, corrupted key pairs, change in site ownership, or suspected fraud.

To obtain the digital certificate, click on the *PICK-UP ID* option from the menu. A form will appear that requires the PIN sent in the notification Email.



Pick Up Digital ID

Important: This step must be completed using the same computer used to submit the enrollment form.
The Personal Identification Number (PIN) is needed to complete this step. It was contained in an e-mail message sent immediately after the enrollment form was submitted.
This was sent by the administrator to the e-mail address entered in the enrollment form.

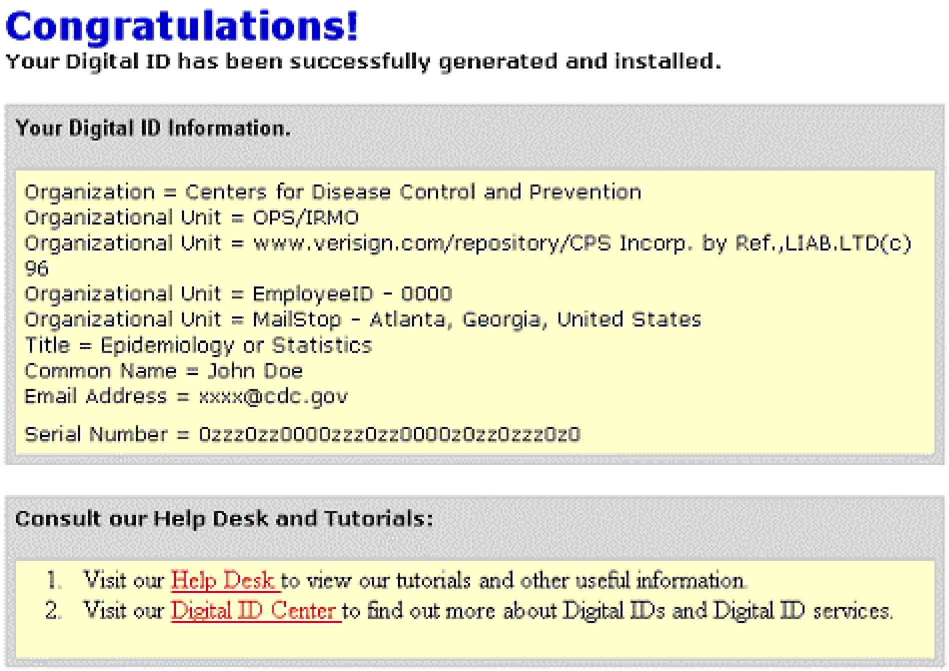
Copy (Ctrl + c) the PIN number from the e-mail, paste (Ctrl + v) it into the box below, and hit SUBMIT.

After the PIN is submitted, generating the Digital ID will take up to three minutes. Do not interrupt the browser until there is a response.

Enter the Personal Identification Number (PIN): The PIN is listed in the confirmation e-mail that was sent from the administrator.	

Once you enter your PIN, click the *Submit* button to download the digital certificate.

If the digital certificate has been successfully installed, a confirmation page with the details of the certificate will be displayed.



Congratulations!

Your Digital ID has been successfully generated and installed.

Your Digital ID Information.

Organization = Centers for Disease Control and Prevention
Organizational Unit = OPS/IRMO
Organizational Unit = www.verisign.com/repository/CPS Incorp. by Ref.,LIAB.LTD(c) 96
Organizational Unit = EmployeeID - 0000
Organizational Unit = MailStop - Atlanta, Georgia, United States
Title = Epidemiology or Statistics
Common Name = John Doe
Email Address = xxxx@cdc.gov

Serial Number = 0zzz0zz0000zzz0zz0000z0zz0zzz0z0

Consult our Help Desk and Tutorials:

1. Visit our Help Desk to view our tutorials and other useful information.
2. Visit our Digital ID Center to find out more about Digital IDs and Digital ID services.

Do not print or disclose the information contained in the confirmation—it is for verification purposes only. The information can be referenced by viewing the details of the digital certificate from the browser.

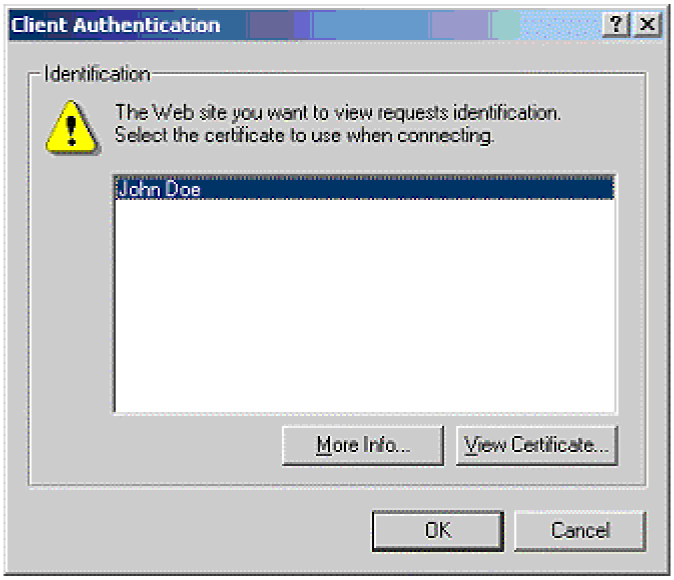
Now you are ready to access the HSVMS. This is done through the CDC's Secure Data Network (SDN).

Accessing SDN

After you obtain and install the digital certificate, you can access the SDN website by going to the following URL:

https://sdn.cdc.gov

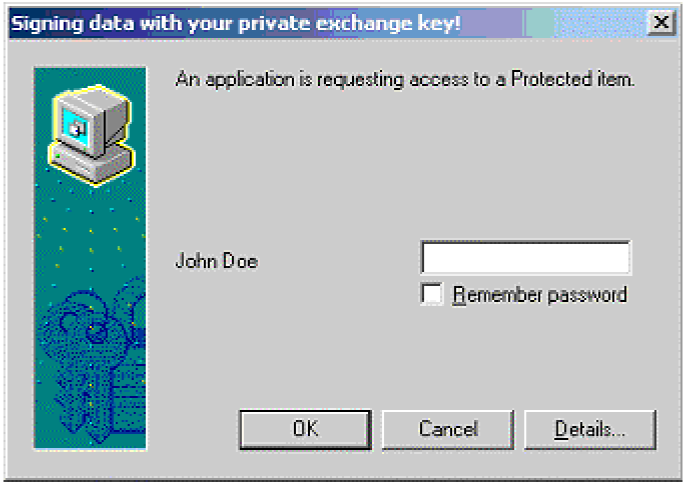
Depending upon the security level of the digital certificate used to access SDN, a user prompt may appear.



The Web site you want to view requests identification.
Select the certificate to use when connecting.

John Doe

Verify the correct digital certificate is being used and click the OK button to continue. If a password is required for use of the digital certificate, a second prompt will appear.



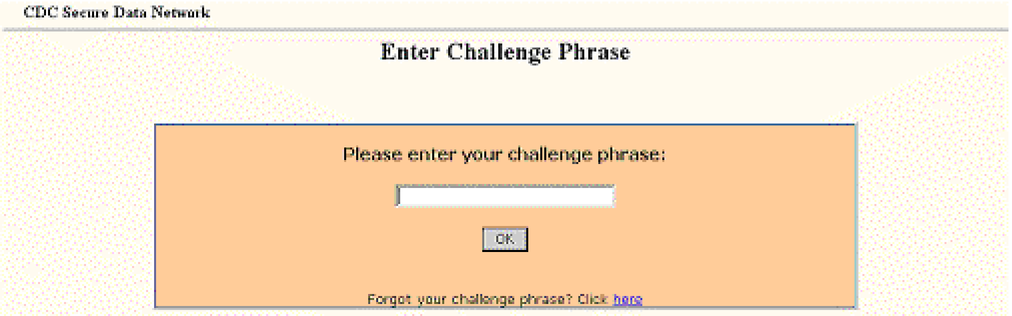
An application is requesting access to a Protected item.

John Doe

□ Remember password

Enter the password you assigned to the digital certificate (not the SDN challenge phrase, unless the same password was used. After entering the password, click the OK button to continue.

After prompting and/or authentication of the digital certificate, the SDN challenge phrase screen will be presented.


CDC Secure Data Network

Enter Challenge Phrase

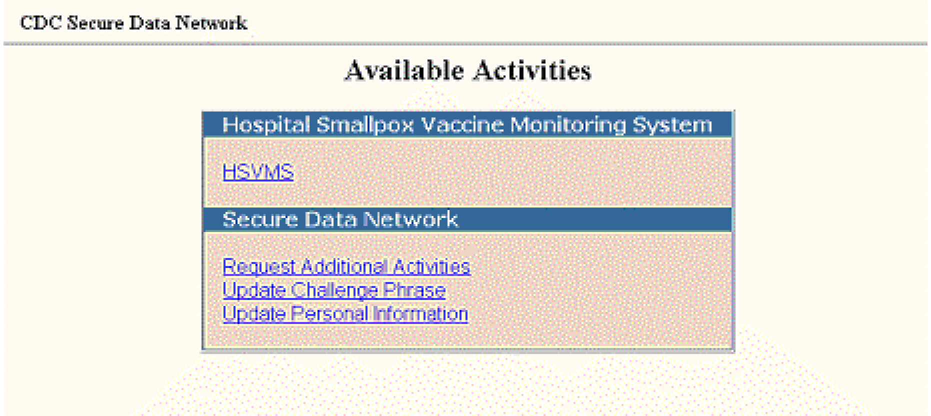
Please enter your challenge phrase:

Forgot your challenge phrase? Click here

Enter the challenge phrase you created when enrolling as an SDN user. After you enter the password, click the OK button to continue.

If you lose or forget the challenge phrase, you can establish a new one by clicking the link provided and entering a replacement. If you request a new challenge phrase, all activities will be disabled and you must be re-approved by the appropriate program administrator.

Once the challenge phrase has been verified, the main SDN page will be displayed providing a list of all available activities. **Choose Hospital Vaccine Safety Monitoring (HSVMS) from the list.**


CDC Secure Data Network

Available Activities

Hospital Smallpox Vaccine Monitoring System

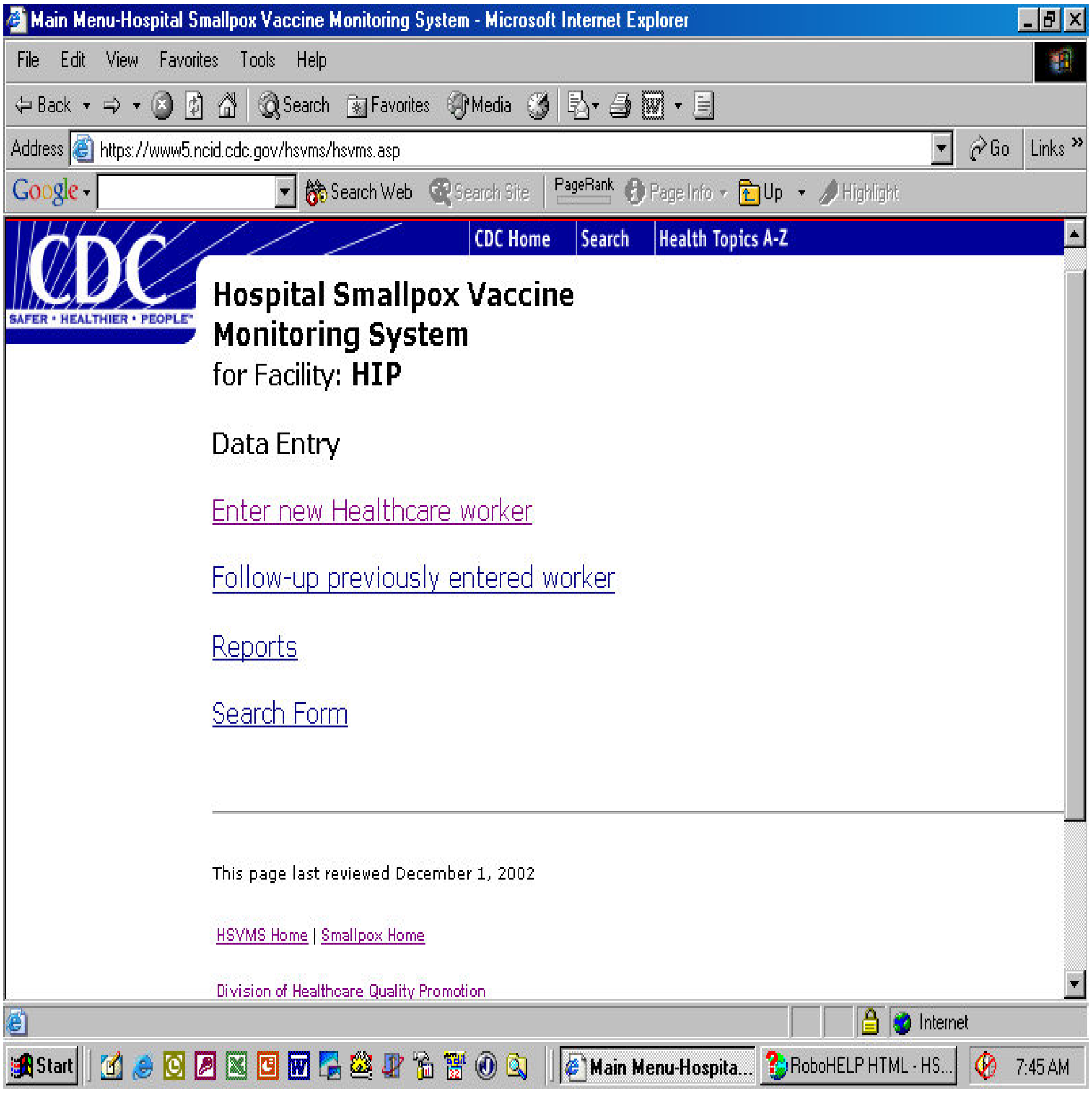
HSVMS

Secure Data Network

Request Additional Activities
Update Challenge Phrase
Update Personal Information

You will be presented with a Facility login screen to enter the facility password that was created upon enrollment to HSVMS.

Enter the facility password, click on Login, and the HSVMS main menu will be displayed.


Main Menu-Hospital Smallpox Vaccine Monitoring System - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://www5.ncid.cdc.gov/hsvms/hsvms.asp
Go Links
Google Search Web Search Site PageRank Page Info Up Highlight
CDC SAFER • HEALTHIER • PEOPLE
CDC Home Search Health Topics A-Z
Internet
Start
Main Menu-Hospita...
RoboHELP HTML - HS...
7:45 AM

Hospital Smallpox Vaccine Monitoring System
for Facility: **HIP**

Data Entry

Enter new Healthcare worker

Follow-up previously entered worker

Reports

Search Form

This page last reviewed December 1, 2002

HSVMS Home | Smallpox Home

Division of Healthcare Quality Promotion

If you have any questions or problems with HSVMS, please contact DHQP at 1-800-893-0485 or 404-498-1250. You may also send us an email:

For help with enrollment: HSVMSenroll@cdc.gov

For help with the software or for content questions after enrolling: HSVMSsupport@cdc.gov